R 032204Z JAN 14
FM COMDT COGARD WASHINGTON DC//CG-112//
TO AIG 4905
BT
UNCLAS //N06010//
SUBJ: GUIDANCE ON EMAILING PROTECTED HEALTH INFORMATION (PHI) A. COMDT COGARD WASHINGTON DC 111751Z DEC 13/AIG 4905 B. COMDT COGARD WASHINGTON DC 241814Z DEC 13/ALCOAST 549/13 C. Coast Guard Security and Information Assurance, COMDTINST
M5500.13 (SERIES)
D. Coast Guard Medical Manual, COMDTINST M6000.1 (SERIES) 1. Cancel REF A.
2. Emails containing Personally Identifiable Information (PII) can be sent freely to recipients with a uscg.mil email address and a need to know.
3. Sensitive Personally Identifiable Information (SPII) includes PHI. SPII is defined as PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. All emails containing PHI, to include inpatient hospitalization messages, shall comply with REFS B and C:
    a. For emails containing PHI sent inside the CG Network - CG personnel are authorized to e-mail PHI freely to recipients with a uscg.mil email address and having a need to know, however, it is strongly encouraged emails and/or attachments be encrypted. In addition, emails containing PHI shall always be digitally signed.
    b. For emails containing PHI sent outside the CG Network - insert the sensitive information into an electronic file, password protect the file, and attach it to the digitally signed email. The password shall be sent via a separate e-mail with a different subject line.
4. Extreme caution shall be used when emailing PHI to a distribution group. The sender shall ensure all recipients included in the distribution group have a "need to know" and follow steps outlined in paragraphs 3.a. or 3.b. above.
5. Per REF B, PII/SPII may be stored on CG shared drives only if access is restricted to those with a need to know by permissions settings or passwords. This also applies to information stored on CGPortal.
6. A user guide on how to digitally sign and encrypt emails, and how to encrypt documents is available at the following link: https://cglink.uscg.mil/1810db85. It is highly recommended all users sending PHI become familiar with the guide.
7. TISCOM is currently testing a solution that will enable access to encrypted email on mobile devices running GOOD Mobile Messaging (GMM). Estimated deployment is spring 2014.
8. This change will be updated in the next version of REF D.
9. POC: CDR Aaron Middlekauff COMDT (CG-1122), 202-475-5185
Email: Aaron.P.Middlekauff(AT)uscg.mil.
10. Released by CAPT Erica Schwartz, Chief, Office of Health Services
11. Internet release is authorized.
BT
NNNN